ПРОТОКОЛ № 27171/2025

проведения совместных испытаний программного обеспечения "Positive Technologies Network Attack Discovery" версии 12.2 и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7)

г. Казань 26.02.2025

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 18.02.2025 по 26.02.2025 совместных испытаний программного обеспечения "Positive Technologies Network Attack Discovery" версии 12.2 (далее – ПО), разработанного АО "Позитив Текнолоджиз", и операционной системы специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2024-0830SE17 (оперативное обновление 1.7.6) (далее – Astra Linux SE 1.7.6), разработанной ООО "РусБИТех-Астра".

2 Объект испытаний

2.1 Перечень компонентов, эксплуатировавшихся в ходе проведения данных испытаний, относящихся к ПО, представлен в Таблице 1.

Таблица 1 – Перечень компонентов, относящихся к ПО

Описание	**Наименование**	**MD5**	**Источник**
Файл архива дистрибутива ПО	ptnad-installer.12.2.1050.tar.gz	f93ffa01f95fdade17c7b1ef1f9fb390	Сторона разработчика ПО
Файл архива, содержащий зависимости ПО	ptnad-depends.12.2.1050.tar.gz	05f0ecac15352455a3175a25789d8c40	Сторона разработчика ПО
Официальное руководство администратора ПО	pt_nad_12.2_adminguide_ru_20250128.pdf	dc33fe47bc05dc3aa075fe8ad6777491	Сторона разработчика ПО
Официальное руководство пользователя ПО	pt_nad_12.2_operatorguide_ru_20250128.pdf	44e127798218135e8d71b7205579c407	Сторона разработчика ПО

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки корректности функционирования ПО в среде Astra Linux SE 1.7.6 в объеме, указанном в Приложении 1.

3.2 Перечень используемых репозиториев приведен в Приложении 2.

3.3 С целью проведения проверок при включённом режиме ЗПС в ходе внедрения ЭЦП в ELF/PE32-файлы ПО использовался комплект цифровых ключей программы Ready for Astra

3.4 При функционировании ПО выявлены ошибки DIGSIG, что является признаком некорректной работы ПО с активным режимом ЗПС. Данные ошибки вызваны запуском созданных во время установки исполняемых файлов. Установка при этом завершается с ошибкой.

3.5 Проверка корректности функционирования ПО в условиях ненулевого уровня конфиденциальности механизма мандатного разграничения доступа (далее – МРД) указанных сред не проводилась по причине отсутствия поддержки ПО соответствующей функциональности ОС. Информация об отсутствии упомянутой поддержки была заявлена стороной разработчика ПО.

3.6 Для успешной установки ПО необходимо отключить механизм МРД.

3.7 При установке и эксплуатации ПО не выполняются условия п. 17.3.1.9 "Руководство по КСЗ Ч. 1". Вносятся изменения в системное время.

3.8 При установке и эксплуатации ПО не выполняются условия п. 17.2.1.5 "Руководство по КСЗ Ч. 1". В среду ОС привносятся внешний модули ядра igb_uio, провести контроль целостности такого модуля в рамках Испытаний не представляется возможным.

3.9 Установка ПО в среде Astra Linux SE 1.7.6 с ядрами hardened завершается с ошибкой: Job for redis-server.service failed because the control process exited with error code.

4 Результаты испытаний

4.1 ПО корректно функционирует в среде Astra Linux SE 1.7.6.

5 Вывод

5.1 ПО и операционная система специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) совместимы, принимая во внимание информацию, содержащуюся в разделах 3, 4 и Приложении 2.

6 Состав рабочей группы и подписи сторон

6.1 Данный протокол составлен участниками рабочей группы:

Карпенко Д. И. – начальник сектора, ООО "РусБИТех-Астра";

Поликаров Е. А. – инженер, ООО "АйСиЭл Астра Сервис".

Приложение 1 к Протоколу № 27171/2025

Перечень проверок совместимости ПО и Astra Linux SE 1.7.6

№ п/п	Наименование проверки	Результат проверки ПО и Astra Linux SE 1.7.6 с ядром ОС							
		5.4.0-186-generic	5.4.0-186-hardened	5.10.216-1-generic	5.10.216-1-hardened	5.15.0-111-generic	5.15.0-111-hardened	5.15.0-111-lowlatency	6.1.90-1-generic
1.	Установка ПО	Успешно	Неуспешно	Успешно	Неуспешно	Успешно	Неуспешно	Успешно	Успешно
2.	Эксплуатация ПО	Успешно	Не проводилась	Успешно	Не проводилась	Успешно	Не проводилась	Успешно	Успешно
3.	Удаление ПО	Успешно	Не проводилась	Успешно	Не проводилась	Успешно	Не проводилась	Успешно	Успешно
4.	Требования безопасности ALSE	Неуспешно	Не проводилась	Неуспешно	Не проводилась	Неуспешно	Не проводилась	Неуспешно	Неуспешно
5.	Механизм безопасности ЗПС	Неуспешно	Не проводилась	Неуспешно	Не проводилась	Неуспешно	Не проводилась	Неуспешно	Неуспешно
6.	Механизм безопасности МКЦ	Успешно	Не проводилась	Успешно	Не проводилась	Успешно	Не проводилась	Успешно	Успешно
7.	Механизм безопасности МРД	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась

Приложение 2 к Протоколу № 27171/2025

Инструкция по установке и удалению ПО в среде Astra Linux SE 1.7.6

1 Используемые репозитории:

в Astra Linux SE 1.7.6:

- deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-base/ 1.7_x86-64 main contrib non-free
- deb [trusted=yes] file:/home/u/ptnad-installer/ptnad-distrib ./
- deb [trusted=yes] file:/home/u/ptnad-installer/repos/additional_packages ./
- deb [trusted=yes] file:/home/u/ptnad-installer/repos/astra_1.7_x86-64 ./

2 Установка ПО:

2.1 выполнить системные команды, действия:

На ВМ должны присутствовать минимум 2 сетевых интерфейса.

Удалить network-manager:
sudo apt remove -y network-manager

Настроить сеть (например, через /etc/network/interfaces)

Отключить механизм МРД:
sudo astra-mac-control disable

Выполнить перезагрузку.

Проверить доступа к серверу обслуживания PT NAD:
wget -Sq -O /dev/null https://update.ptsecurity.com/test

Скопировать архивы дистрибутива ПО в директорию (например ptnad-installer) и распаковать их:
cd ./ptnad-installer
tar pxf ptnad-installer.12.2.1050.tar.gz
tar pxf ptnad-depends.12.2.1050.tar.gz

Установите пакет linux-headers, соответствующий версии ядра Linux:
sudo apt install linux-headers-$(uname -r)

Установить postgresql-11:
sudo apt install -y postgresql-11

Запустить установку ПО:
sudo ./install.sh

- Выберите язык мастера установки English и нажмите клавишу Enter.
- Подтвердите ознакомление с лицензионным соглашением, выбрав Ok и нажав клавишу Enter.
- Примите условия лицензионного соглашения, выбрав Yes и нажав клавишу Enter.

- Выберите All-in-One PT NAD и нажмите клавишу Enter.
- На следующих этапах нажимайте клавишу Enter, сохраняя параметры по умолчанию.
- Если для захвата трафика не планируется использовать интерфейсы сетевой карты NVIDIA Mellanox, выберите No и нажмите клавишу Enter.

Запустите мастер настройки PT NAD выполнив команду:
sudo nad-configure

- В открывшемся окне мастера настроек выберите Continue и нажмите клавишу Enter.
- Не заполняйте поле System tag, выберите Next и нажмите клавишу Enter.
- Выберите интерфейс управления. Перейдите к следующему шагу выбрав Next.
- Оставьте настройки Elasticsearch (CPU and RAM, traffic metadata storage time and number of online shards) по умолчанию и перейдите к следующему шагу выбрав Next.
- Выберите интерфейс, с которого модуль ptdpi должен захватывать трафик (интерфейс, выбранный в качестве интерфейса управления, не использовать) – после чего Next
- Выберите механизм захвата трафика DPDK – после чего Next
- Значение в поле Capture MTU оставьте по умолчанию - после чего Next
- Выберите расчетную скорость захвата трафика в организации, после чего — вариант Next.
- Оставьте поле IP address пустым и выберите вариант Next.
- Подтвердите настройки – выберите Save and exit и нажмите клавишу Enter.
- Reboot the system -> Yes -> Enter

После установки PT NAD 12.2 запустите скрипт для переноса параметров продукта из конфигурационных файлов в базу данных:
sudo /opt/ptsecurity/nad/bin/manage settings migrate

3 Удаление ПО:

3.1 выполнить системную команду:

sudo ./uninstall.sh

Приложение 3 к Протоколу № 27171/2025

Перечень используемых сокращений

Astra Linux SE 1.7.6 – операционная система специального назначения "Astra Linux Special Edition" РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2024-0830SE17 (оперативное обновление 1.7.6);

ЗПС – замкнутая программная среда;

МКЦ – мандатный контроль целостности;

МРД – мандатное управление доступом;

ОС – операционная система;

"Руководство по КСЗ Ч. 1" – документ "Операционная система специального назначения "Astra Linux Special Edition". Руководство по КСЗ. Часть 1" РУСБ.10015-01 97 01-1;

ПО – программное обеспечение "Positive Technologies Network Attack Discovery" версии 12.2.